SEMICONDUCTOR STORAGE DEVICE AND DATA PROCESSOR

Patent Number: JP9069067

Publication date: 1997-03-11

Inventor(s): NAKAMURA YASUHIRO; FURUSAWA KAZUNORI; ETO JUN; IZAWA KAZUTO; YUGAWA YOSUKE; KOSAKAI KENJI

Applicant(s): HITACHI LTD

Requested Patent: ☐ JP9069067

Application Number: JP19950246956 19950831

Priority Number(s):

IPC Classification: G06F12/14; G11C16/06

EC Classification:

Equivalents:

Abstract

PROBLEM TO BE SOLVED: To actualize a security protecting function in a semiconductor memory chip by comparing a password written in a register with an externally inputted password and deciding whether or not a read of data from a memory cell array is allowed.

SOLUTION: The semiconductor storage device is constituted including the register 20 where a password can be set, a password deciding means which decides whether or not the password set in the register 20 matches an externally inputted password, and a control means which allows or inhibit a data read from the memory cell array 13 according to the decision result of the password deciding means. Then this control means allows or inhibits the data read from the memory cell array 13 according to the decision result showing whether or not the password set in the register 20 matches the externally inputted password. Thus, the security protecting function is displayed in the semiconductor storage device.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－69067

(43)公開日　平成９年(1997)３月11日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　12/14	３２０		Ｇ０６Ｆ　12/14	３２０Ｃ	
Ｇ１１Ｃ　16/06			Ｇ１１Ｃ　17/00	３０９Ｆ	

審査請求　未請求　請求項の数５　ＦＤ　（全 10 頁）

(21)出願番号　特願平7－246956

(22)出願日　平成７年(1995)８月31日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　中村　靖宏
東京都小平市上水本町５丁目20番１号　株式会社日立製作所半導体事業部内

(72)発明者　古沢　和則
東京都小平市上水本町５丁目20番１号　株式会社日立製作所半導体事業部内

(72)発明者　衛藤　潤
東京都小平市上水本町５丁目20番１号　株式会社日立製作所半導体事業部内

(74)代理人　弁理士　玉村　静世

最終頁に続く

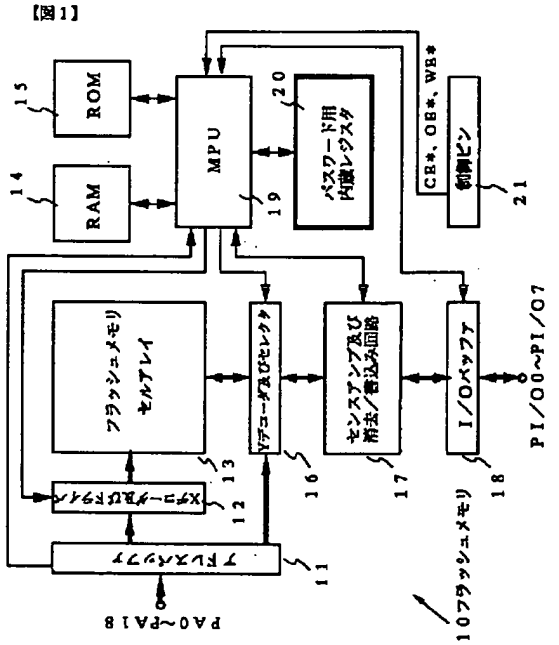
(54)【発明の名称】　半導体記憶装置、及びデータ処理装置

(57)【要約】

【目的】　本発明の目的は、半導体記憶装置の内部に機密保護機能を搭載するための技術を提供することにある。

【構成】　パスワード用内蔵レジスタ２０に設定されたパスワードと、外部から入力されたパスワードとが一致するか否かが判定され、その判定結果に基づいて、フラッシュメモリセルアレイ１３からのデータ読出しを許容又は禁止するようにして、メモリＬＳＩ自体で、不正ユーザに対する機密保護を図る。

【図１】



【特許請求の範囲】
【請求項１】　複数のメモリセルを配列して成るメモリセルアレイを含む半導体記憶装置において、
パスワードを設定可能なレジスタと、
上記レジスタに設定されたパスワードと、外部から入力されたパスワードとが一致するか否かを判定するパスワード判定手段と、
上記パスワード判定手段の判定結果に基づいて、上記メモリセルアレイからのデータ読出しを許容又は禁止する制御手段とを含むことを特徴とする半導体記憶装置。
【請求項２】　上記レジスタへのパスワード設定が成功したか否かの情報を外部出力可能な外部ピンを含む請求項１記載の半導体記憶装置。
【請求項３】　上記レジスタへの不適切なパスワード書込みの回数を計数する第１計数手段と、
上記第１計数手段の計数結果が、所定値に達したか否かを判定するための第１計数値判定手段と、
上記計数手段の計数結果が所定値に達した場合の処理を、フラグ状態に基づいて決定するための第１フラグ判定手段とを含む請求項１又は２記載の半導体記憶装置。
【請求項４】　パスワードの誤入力回数を計数する第２計数手段と、
上記第２計数手段の計数結果が、所定値に達したか否かを判定する第２計数値判定手段と、
上記第２計数手段の計数結果が所定値に達した場合の処理を、フラグ状態に基づいて決定するための第２フラグ判定手段とを含む請求項１乃至３のいずれか１項記載の半導体記憶装置。
【請求項５】　請求項１乃至４のいずれか１項に記載の半導体記憶装置と、それをアクセス可能な中央処理装置とを含むデータ処理装置。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、半導体記憶装置、さらにはそれにおける機密保護技術に関し、例えばフラッシュメモリ及びそれを含むデータ処理装置に適用して有効な技術に関する。
【０００２】
【従来の技術】特開平２－２８９９９７号には一括消去型ＥＥＰＲＯＭ（エレクトリカリ・イレーザブル・アンド・プログラマブル・リード・オンリ・メモリ）について記載されている。この一括消去型ＥＥＰＲＯＭは、本明細書におけるフラッシュメモリと同意義に把握することができる。フラッシュメモリは、電気的な消去・書込みによって情報を書換え可能であって、ＥＰＲＯＭ（エレクトリカリ・プログラマブル・リード・オンリ・メモリ）と同様に、そのメモリセルを１個のトランジスタで構成することができ、メモリセルの全てを一括して、またはメモリセルのブロックを一括して電気的に消去する機能を持つ。したがって、フラッシュメモリは、システムに実装された状態でそれの記憶情報を書換えることができると共に、その一括消去機能により書換え時間の短縮を図ることができ、さらに、チップ占有面積の低減にも寄与する。
【０００３】フラッシュメモリセルは、フローティングゲートとコントロールゲートの２層構造を持ち、ＥＰＲＯＭとほぼ同じ１トランジスタ型セルとされる。書込みは、ＥＰＲＯＭと同様にコントロールゲート、ドレインに高電圧を印加して、ドレイン接合付近で発生したホットエレクトロンをフローティングゲートに注入して、しきい値を高い状態にすることによって行われる。また、消去は、ソースに高電圧を印加するとともに、コントロールゲートを負電位、若しくは０Ｖに接地し、トンネル現象により、フローティングゲート内の電子をソースに引抜いて、しきい値を低い状態にすることで実現される。
【０００４】
【発明が解決しようとする課題】ところで、上記フラッシュメモリは不揮発性メモリであり、また、オンボード書込みが可能とされることから、プログラムメモリなどとして用いられる。その場合に、記憶されたプログラムを不正ユーザから守るため、機密保護が必要とされる。
【０００５】しかしながら、半導体メモリチップ自体には、機密保護についての機能が搭載されていないために、上記機密保護は、例えば半導体メモリチップの外部においてシステム的に実現する必要がある。半導体メモリチップの外部においてシステム的に実現する場合には、機密保護のための回路ブロックを半導体メモリチップとは別に形成する必要があるから、それにより、ボード上の半導体チップの数が増加してしまうことや、システム構成の複雑化を招くなどの不都合がある。
【０００６】さらに、半導体メモリチップ自体に機密保護機能を搭載することについて本願発明者が検討したところ、内部レジスタ等にパスワードの登録が必要であり、しかも、登録が終了したか否かを外部より確認する必要があることからパスワードの外部読出し機能が必要と考えられる。しかしながら、このパスワードの外部読出し機能を搭載した場合には、第三者によってパスワードレジスタの内容が読出される虞があり、そうすると、機密保護が不十分となってしまい、その点の考慮が必要とされる。
【０００７】本発明の目的は、半導体記憶装置の内部に機密保護機能を搭載するための技術を提供することにある。
【０００８】本発明の前記並びにその他の目的と新規な特徴は本明細書の記述及び添付図面から明らかになるであろう。
【０００９】
【課題を解決するための手段】本願において開示される発明のうち代表的なものの概要を簡単に説明すれば下記

の通りである。

【0010】すなわち、パスワードを設定可能なレジスタ（20）と、このレジスタに設定されたパスワードと、外部から入力されたパスワードとが一致するか否かを判定するパスワード判定手段（19f）と、このパスワード判定手段の判定結果に基づいて、メモリセルアレイからのデータ読出しを許容又は禁止するための制御手段（19j）とを含んで半導体記憶装置を形成する。

【0011】このとき、上記レジスタへのパスワード設定が成功したか否かの情報を外部ピン（PI／O7）を使用して外部出力可能に構成することができる。

【0012】また、上記レジスタへの不適切なパスワード書込みの回数を計数する第1計数手段（19b）と、この第1計数手段の計数結果が、所定値に達したか否かを判定するための第1計数値判定手段（19c）と、第1計数手段の計数結果が所定値に達した場合の処理を、フラグ状態に基づいて決定するための第1フラグ判定手段（19d）とを設けることができる。

【0013】さらに、パスワードの誤入力回数を計数する第2計数手段（19g）と、この第2計数手段の計数結果が、所定値に達したか否かを判定するための第2計数値判定手段（19h）と、第2計数手段の計数結果が所定値に達した場合の処理を、フラグ状態に基づいて決定するための第2フラグ判定手段（19i）とを設けることができる。

【0014】そして、上記構成の半導体記憶装置（19）と、それをアクセス可能な中央処理装置（31）とを含んでデータ処理装置を構成する。

【0015】

【作用】上記した手段によれば、制御手段は、レジスタに設定されたパスワードと、外部から入力されたパスワードとが一致するか否かの判定結果に基づいて、メモリセルアレイからのデータ読出しを許容又は禁止する。このことが、半導体記憶装置内部において機密保護機能を発揮する。

【0016】

【実施例】図7には本発明の一実施例であるフラッシュメモリを含むデータ処理装置が示される。

【0017】このデータ処理装置は、特に制限されないが、システムバスBUSを介して、CPU（中央処理装置）31、フラッシュメモリ10、SRAM（スタティック・ランダム・アクセス・メモリ）33、ROM（リード・オンリ・メモリ）34、周辺装置制御部35、表示制御部36などが、互いに信号のやり取り可能に結合され、予め定められたプログラムに従って所定のデータ処理を行うコンピュータシステムとして構成される。上記CPU30は、本システムの論理的中核とされ、主として、アドレス指定、情報の読出しと書込み、データの演算、命令のシーケンス、割り込の受付け、記憶装置と入出力装置との情報交換の起動等の機能を有し、演算制御部や、バス制御部、メモリアクセス制御部などから構成される。フラッシュメモリ10や、SRAM33、及びROM34は内部記憶装置として位置付けられ、他の電子部品とともに、ボードに搭載されている。

【0018】フラッシュメモリ10には、オペレーティングシステム（OS）のコアの一部などが格納されている。フラッシュメモリ10に格納されるOS部分は、OSのバージョンアップなどによって変更される可能性があるため、それに対処するには、記憶内容のオンボード書換えが可能なフラッシュメモリ10が好適とされる。そして、このフラッシュメモリ10には、記憶情報を不正ユーザから守るため、後に詳述するように、記憶内容の機密保護機能が備えられている。

【0019】また、SRAM33には、CPU30での計算や制御に必要なプログラムやデータが格納される。周辺装置制御部35によって、外部記憶装置38の動作制御や、キーボード39などからの情報入力制御が行われ、上記表示制御部36によって、CRTディスプレイ40への情報表示制御が行われる。

【0020】図1には上記フラッシュメモリ10の構成例が示される。

【0021】図1に示されるフラッシュメモリ10は、特に制限されないが、公知の半導体集積回路製造技術により、単結晶シリコン基板などの一つの半導体基板に形成される。

【0022】8ビットのデータ入出力ピンPI／O0～PI／O7、19ビットのアドレス入力ピンPA0～PA18、さらにはチップイネーブル信号CE＊、アウトプットイネーブル信号OE＊、ライトイネーブル信号WE＊の各種制御信号の入力ピンを含む制御ピン21が設けられている。尚、図示されないが、5Vのような高電位側電源端子、0Vのような低電位側電源端子、及び12Vのような高電圧端子が設けられている。

【0023】13は、それぞれ2層ゲート構造の絶縁ゲート型電界効果トランジスタによって構成された複数のフラッシュメモリセルをマトリクス配置して成るフラッシュメモリセルアレイである。フラッシュメモリセルのコントロールゲートはそれぞれ対応する図示しないワード線に接続され、フラッシュメモリセルのドレインはそれぞれ対応する図示しないデータ線に接続され、フラッシュメモリセルのソースはメモリブロック毎に共通の図示しないソース線に接続されている。

【0024】アドレスバッファ11は、アドレス入力ピンPA0～PA18から供給されるアドレス信号を内部相補アドレス信号に変換する。変換されたアドレス信号は、アドレスラッチなどを介して、後段のXデコーダ及びドライバ12、及びYデコーダ及びセレクタ16に伝達される。Xデコーダ及びドライバ12は入力されたXアドレス信号を解読し、解読して得られる選択信号などに基づいてワード線を駆動する。データ読出し動作には

ワード線に５Ｖのような電圧が供給される。データの書込み動作においては、ワード線に１２Ｖのような高電圧が供給される。データの消去動作においては、Ｘデコーダ及びドライバ１２の全ての出力は０Ｖのような低い電圧レベルにされる。

【００２５】Ｙデコーダ及びセレクタ１６は、入力されたＹアドレス信号を解読し、それに基づいてデータ線を選択する。データ読出し動作において、上記Ｙデコーダ及びセレクタ１６で選択されたデータ線からの読出し信号を増幅するセンスアンプ及び消去／書込み回路１７が設けられ、また、データを外部に出力するためのデータ出力バッファや、外部から供給される書込みデータ又はコマンドデータなどを取り込むためのデータ入力バッファを含むＩ／Ｏバッファ１８が設けられる。

【００２６】上記Ｉ／Ｏバッファ１８を介して取込まれたコマンドデータは、ＭＰＵ１９に供給される。ＭＰＵ１９には、予め設定されたパスワードを保持するパスワード用内蔵レジスタ２０、ＲＡＭ１４、ＲＯＭ１５が結合されている。ＭＰＵ１５は、その他に制御ピン２１を介して供給されるチップイネーブル信号ＣＥ＊、アウトプットイネーブル信号ＯＥ＊、及びライトイネーブル信号ＷＥ＊などを受け、フラッシュメモリの読出し、消去、書込み動作、書込みベリファイなどの各種内部動作を、ＲＯＭ１５に格納されたプログラムに従って制御する。そのような制御動作において、上記ＲＡＭ１４は、ＭＰＵ１９における処理の作業領域等に使用される。また、上記パスワード用内蔵レジスタ２０へのパスワード書込みは可能とされるが、このパスワード用内蔵レジスタ２０に登録されたパスワードそのものを外部に出力するためのパスは設けられていない。つまり、フラッシュメモリ１０の機密保護の確実化を図るため、パスワード用内蔵レジスタ２０に登録されたパスワードの外部読出しが不可能とされている。

【００２７】図２には、上記ＭＰＵ１９における主要機能ブロックが示される。

【００２８】図２に示されるように、ＭＰＵ１９は、パスワード設定系機能ブロック１９１と、パスワード判定系機能ブロック１９２とを含み、それらはＭＰＵ１９で所定のプログラムが実行されることによって実現される。

【００２９】パスワード設定系機能ブロック１９１には、パスワード書込みのための手続が正しく行われたか否かを判定するための手続き判定手段１９ａ、パスワード書込みのための手続が不適切であった場合の回数を計数するための計数手段１９ｂ、この計数値によって計数された値（これをｔで示す）が、所定回数（これをｎで示す）に達したか否かを判定するための計数値判定手段１９ｃ、計数手段１９ｂの計数結果が所定値に達した場合の処理を、フラグ状態に基づいて決定するためのフラグ判定手段１９ｄ、及び上記手続き判定手段１９ａやフラグ判定手段１９ｄの判定結果に基づいてパスワード書込に関する制御を行うパスワード書込み制御手段１９ｅが含まれる。

【００３０】パスワード判定系ブロック１９２には、入力されたパスワードが、パスワード用内蔵レジスタ２０に設定されたパスワードと一致するか否かを判定するためのパスワード判定手段１９ｆ、パスワードの誤入力回数（これをｋで示す）を計数するための計数手段１９ｇ、このパスワード誤入力回数ｋが、所定値ｎに達したか否かを判定するための計数値判定手段１９ｈ、計数手段１９ｇの計数結果が所定値ｎに達した場合の処理を、フラグ状態に基づいて決定するためのフラグ判定手段１９ｉ、及び上記パスワード判定手段１９ｆやフラグ判定手段１９ｉの判定結果に基づいてフラッシュメモリセルアレイ１３の記憶情報の読出しに関する制御を行うアクセス制御手段１９ｊが含まれる。

【００３１】ここで、上記計数値判定手段１９ｃ，１９ｈにおいて参照される所定値ｎは、特に制限されないが、「３」とされる。また、上記フラグ状態とは、フラッシュメモリ１０のウェーハプロセス段階、又はウェーハプローピング段階でのヒューズ回路への書込みによって設定されたフラグの論理状態であり、通常はユーザ仕様に応じて、その論理状態が決定される。

【００３２】パスワード設定（登録）について詳述する。

【００３３】図３及び図４にはパスワード設定に関する動作タイミングが示される。

【００３４】図３に示されるように、パスワードの登録は、チップイネーブル信号ＣＥ＊がローレベルにアサートされた状態で、ライトイネーブル信号ＷＥ＊がローレベルにアサートされるタイミングに同期して行われる。つまり、ライトイネーブル信号ＷＥ＊がローレベルにアサートされるタイミングに同期して、パスワード設定のためのコマンド及びパスワードが入力される。このコマンド及びパスワードは、データ入出力ピンＰＩ／Ｏ０～ＰＩ／Ｏ６を介して行われる。データ入出力ピンＰＩ／Ｏ７がローレベルの期間が、パスワード登録中であることを示している。そして、このパスワード登録直後に、データ入出力ピンＰＩ／Ｏ７がハイレベルにされた場合には、登録が正常に行われたことを示している（登録成功）。それに対して、図４に示されるように、パスワード登録直後にデータ入出力ピンＰＩ／Ｏ７がハイレベルにされない場合には、パスワードの登録が正常に行われていないことを示している（登録失敗）。このように、パスワードが正常に設定されたか否かの情報がデータ入出力ピンＰＩ／Ｏ７に表れるようになっており、それにより、パスワード設定に関するチェックが可能とされるので、パスワード用内蔵レジスタ２０からパスワード自体の読出しを行う必要が無い。このため、パスワード用内蔵レジスタ２０からパスワードを読出すためのパスは

形成されていない。

【００３５】図５にはパスワード用内蔵レジスタ２０へのパスワード書込みについての処理の流れが示される。

【００３６】パスワード登録のためのコマンド入力、パスワード入力等、パスワード用内蔵レジスタ２０へのパスワード書込みのための所定の手続が行われると（ステップＳ３１）、その手続きが正しいか否かの判別が手続き判定手段１９ａによって行われる（ステップＳ３２）。図３に示されるように、パスワード書込みのための所定の手続が正く行われた場合（ＹＥＳ）、パスワード書込み制御手段１９ｅによって、パスワード用内蔵レジスタ２０へのパスワード書込みが許容される（ステップＳ３７）。そして、パスワード登録が正常に行われた場合には、アウトプットイネーブル信号ＯＥ＊がローレベルにされた期間において、データ入出力ピンＰＩ／Ｏ７がハイレベルにされることによって、登録成功が示される。また、ステップＳ３２の判別において、手続きが正しくないと判断された場合（ＮＯ）には、そのような不適切な手続き回数ｔが計数手段１９ｂによってインクリメントされる（ステップＳ３３）。不適切な手続き回数ｔの値は、フラッシュメモリセルアレイ１３の一部を利用して形成された回数記憶領域、あるいはＭＰＵ１９の内部に形成される適宜の不揮発性記憶領域に書込まれる。不揮発性領域に、不適切な手続き回数ｔが記憶されるため、回数ｔはシステムの電源を再投入した場合でも初期化されない。そして、上記ステップＳ３３の不適切な手続き回数ｔのインクリメントが行われた後に、この回数ｔが所定値ｎに達したか否かの判別が計数値判定手段１９ｃによって行われる（ステップＳ３４）。本実施例においては、特に制限されないが、ｎ＝３と設定されているから、上記ステップＳ３４の判別においては、不適切な手続き回数ｔが３になったか否かの判別が行われる。この判別において、不適切な手続き回数ｔが未だ３に達していないと判断された場合（ＮＯ）には、再びパスワードの書込み待ち状態となり、パスワードの再書込みが可能とされる。しかし、上記ステップＳ３４の判別において、不適切な手続き回数ｔが３に達したと判断された場合（ＹＥＳ）には、フラグＦＬＧ１の設定状態がチェックされる（ステップＳ３５）。つまり、フラグＦＬＧ１＝０が成立するか否かの判別が行われる。フラグＦＬＧ１は、上記のように、フラッシュメモリ１０のウェーハプロセス段階、又はウェーハプロービング段階でのヒューズ回路への書込みによって設定されている。ユーザによるパスワード書込み手続きが正しく行われなかった場合に、フラッシュメモリ１０をどのような状態にするかは、ユーザオプションとされている。例えば、機密保護をより完璧なものとするため、不適切なパスワード書込み手続き回数ｔが３に達した場合に、二度とパスワード設定ができない状態とする第１方式を選択するユーザに対しては、上記フラグＦＬＧ１は、「０」に設定される。それに対して、不適切なパスワード書込み手続き回数ｔが３に達した場合でも、再びパスワード書込み手続が行えるようにする第２方式を選択するユーザに対しては、上記フラグＦＬＧ１は、「１」に設定される。ステップＳ３５の判別において、ＦＬＧ１＝０が成立すると判断された場合（ＹＥＳ）には、フラッシュメモリ１０は二度とパスワード設定ができない状態にされる（ステップＳ３６）。そのような状態は、書込み処理についての所定のベクタテーブルへのジャンプが行われないようにすることで、実現される。また、ステップＳ３５の判別において、ＦＬＧ１＝０が成立しないと判断された場合には、再びパスワードの書込み待ち状態となる。

【００３７】ここで、パスワード書込みのための正しい手続が行われる限り、上記ステップＳ３２の判別において手続が正しいと判断されて、何度でもパスワードの再書込みが可能とされると、不正ユーザによってパスワードが変更される虞があるから、フラッシュメモリセルアレイ１３の機密保護に欠ける。そのため、本実施例では、上記ステップＳ３７でパスワード書込みが許容されるのは、１回に制限されている。つまり、正規ユーザによって、正しくパスワードが設定されたなら、それ以降、例え正規ユーザであっても、パスワードの再書込みは不可能となる。そのような制限は、フラッシュメモリセルアレイ１３の機密保護の確実化を達成する上で、非常に有効とされる。

【００３８】図６にはパスワード判定系の処理の流れが示される。

【００３９】フラッシュメモリセルアレイ１３の記憶情報を読出す場合には、パスワード用内蔵レジスタ２０に登録されたパスワードと同一のパスワードが入力されることが条件とされる。パスワードの入力が行われると（ステップＳ４１）、この入力されたパスワードと、パスワード用内蔵レジスタ２０に登録されたパスワードとが一致するか否かの判別がパスワード判定手段１９ｆによって行われる（ステップＳ４２）。この判別において、パスワードが一致すると判断された場合（ＹＥＳ）には、フラッシュメモリセルアレイ１３の記憶情報の読出しが許容される（ステップＳ４７）。しかし、上記ステップＳ４２の判別において、パスワードが一致しないと判断された場合（ＮＯ）には、パスワード誤入力回数ｋの値が計数手段１９ｇによってインクリメントされる（ステップＳ４３）。パスワード誤入力回数ｋの値は、上記不適切な手続き回数ｔの場合と同様に、フラッシュメモリセルアレイ１３の一部を利用して形成された回数記憶領域、あるいはＭＰＵ１９の内部に形成される適宜の不揮発性記憶領域に書込まれる。そのような不揮発性領域に、パスワード誤入力回数ｋが記憶されるため、パスワード誤入力回数ｋはシステムの電源を再投入した場合でも初期化されない。そして、上記ステップＳ４３の

パスワード誤入力回数ｋのインクリメントが行われた後に、この回数ｋが所定値ｎに達したか否かの判別が計数値判定手段１９ｈによって行われる（ステップＳ４４）。例えば、ｎ＝３と設定されている場合には、上記ステップＳ４４の判別においては、パスワード誤入力回数ｋが３になったか否かの判別が行われる。この判別において、パスワード誤入力回数ｋが未だ３に達していないと判断された場合（ＮＯ）には、再びパスワードの入力待ち状態となる。つまり、パスワードの再入力が可能とされる。それは、フラッシュメモリ１０の正規ユーザであっても、パスワードの誤入力は十分に考えられるから、その場合の救済を考慮している。しかし、上記ステップＳ４４の判別において、パスワード誤入力回数ｔが３に達したと判断された場合（ＹＥＳ）には、フラグＦＬＧ２の設定状態がチェックされる（ステップＳ４５）。つまり、フラグＦＬＧ２＝０が成立するか否かの判別が行われる。フラグＦＬＧ２は、上記フラグＦＬＧ１の場合と同様に、フラッシュメモリ１０のウェーハプロセス段階、又はウェーハプローピング段階でのヒューズ回路への書込みによって設定されている。そして、ユーザによるパスワード入力が正しく行われなかった場合に、フラッシュメモリ１０をどのような状態にするかは、ユーザオプションとされる。例えば、機密保護をより完璧なものとするため、パスワード誤入力回数ｋが３に達した場合に、フラッシュメモリ１０を二度と使用できなくする状態を選択するユーザに対しては、上記フラグＦＬＧ２は、「０」に設定される。それに対して、パスワード誤入力回数ｋが３に達した場合でも、再びパスワード入力が行えるようにするのを選択するユーザに対しては、上記フラグＦＬＧ２は、「１」に設定される。ステップＳ３５の判別において、ＦＬＧ２＝０が成立すると判断された場合（ＹＥＳ）には、フラッシュメモリ１０はフラッシュメモリセルアレイ１３の記憶情報の読出しが二度とできない状態にされる（ステップＳ４６）。

【００４０】上記実施例によれば、以下の作用効果を得ることができる。

【００４１】（１）パスワード用内蔵レジスタ２０に設定されたパスワードと、外部から入力されたパスワードとが一致するか否かが判定され、その判定結果に基づいて、フラッシュメモリセルアレイ１３からのデータ読出しを許容又は禁止するようにしているので、メモリＬＳＩ自体で、不正ユーザに対する機密保護を図ることができる。特に、ＬＳＩの着脱の容易化のためにＩＣソケット等によってフラッシュメモリ１０をボードに搭載する場合においても、フラッシュメモリ単体で機密保護機能を発揮することから、オペレーティングシステムのコアの一部など、フラッシュメモリに記憶された情報が不正ユーザによって読出されるのを防止することができる。

【００４２】（２）データ入出力ピンＰＩ／Ｏ７を利用して、パスワード用内蔵レジスタ２０へのパスワード設定が成功したか否かの情報を外部出力することができるので、パスワード設定が行われたか否かの確認のため、パスワード用内蔵レジスタ２０の記憶内容を外部出力する必要が無い。つまり、パスワード用内蔵レジスタ２０に記憶されたパスワードの外部出力のためのパスを形成する必要が無いから、不正ユーザによってパスワードが読出される虞が無い。このことは、機密保護をより確実にする上で有効とされる。

【００４３】（３）パスワード用内蔵レジスタ２０への不適切なパスワード書込みの回数を計数する計数手段１９ｂと、この計数手段１９ｂの計数結果が、所定値に達したか否かを判定するための計数値判定手段１９ｃと、上記計数手段１９ｂの計数結果が所定値に達した場合の処理を、フラグ状態に基づいて決定するためのフラグ判定手段１９ｄとが、ＭＰＵ１９で形成されることにより、メモリＬＳＩにおける機密保護機能のためのパスワード設定を的確に行うことができる。

【００４４】（４）さらに、不正なパスワードの入力回数を計数する計数手段１９ｇと、この計数手段１９ｇの計数結果が、所定値に達したか否かを判定するための計数値判定手段１９ｈと、上記計数手段１９ｇの計数結果が所定値に達した場合の処理を、フラグ状態に基づいて決定するためのフラグ判定手段１９ｉとが、ＭＰＵ１９で形成されることにより、メモリＬＳＩにおける機密保護機能を容易に実現することができる。

【００４５】（５）上記（１）～（４）の作用効果を有するフラッシュメモリ１０と、それをアクセス可能なＣＰＵ３１とを含むデータ処理装置においては、フラッシュメモリ１０自体で機密保護機能が実現されることから、このフラッシュメモリ１０の記憶情報についての機密保護をシステム的に実現する必要が無いので、システム構成の簡略化を図ることができる。

【００４６】図８にはフラッシュメモリの他の構成例が示される。

【００４７】図８に示されるフラッシュメモリ１０には、ＭＰＵ１９の外部に、パスワードの誤入力回数を計数するためのカウンタ５１が設けられている。このカウンタ５１によってパスワードの誤入力回数が計数され、その計数結果が所定値に達したとき、センスアンプ及び消去／書込み回路１７の動作が制限される。つまり、カウンタ５１での計数結果に基づいて、パスワードの誤入力回数が所定値に達した場合、それは当該フラッシュメモリに対する不当なアクセスであると判断して、センスアンプ及び消去／書込み回路１７の動作が制限されることで、フラッシュメモリセルアレイ１３の記憶情報の外部読出しが禁止される。このように、ＭＰＵ１９の外部に、パスワードの誤入力回数を計数するためのカウンタ５１を設け、その計数結果に基づいて、フラッシュメモリセルアレイ１３の記憶情報の外部読出しを禁止するよ

うにしても、上記実施例の場合と同様の作用効果を得ることができる。

【００４８】図９には、本発明の一実施例であるフラッシュメモリの別の適用例が示される。

【００４９】上記実施例では、メモリＬＳＩとしてのフラッシュメモリ１０をデータ処理装置のボードに搭載した場合について説明したが、図９に示されるデータ処理装置は、フラッシュメモリによって形成されたフラッシュメモリカード６５を着脱自在に結合して成る。フラッシュメモリカード６５は、特に制限されないが、中央処理装置（ＣＰＵ）６１と共に、ランダム・アクセス・メモリ（ＲＡＭ）６２やリード・オンリ・メモリ（ＲＯＭ）６３が共通接続されるバス６６に、インタフェース回路（Ｉ／Ｆ）６４を介して接続される。フラッシュメモリカード６５は、適宜のコネクタによって、データ処理システムに着脱自在に装着される。フラッシュメモリカード６５には、ＣＰＵ６１で実行可能な各種プログラムや、各種データ等が記憶されている。データ処理システムに装着された状態で、フラッシュメモリカード６５はホスト装置としてのＣＰＵ６１によってアクセスされる。ＲＯＭ６３には、ＣＰＵ６１で実行されるプログラムが格納される。ＲＡＭ６２は、処理対象とされるデータの一時記憶領域や、ＣＰＵ６１での演算処理の作業領域などとして利用される。

【００５０】上記フラッシュメモリカード６５は、特に制限されないが、ＪＥＩＤＡメモリカード（タイプＩ）、すなわち、ＪＥＩＤＡメモリカードインタフェースに適合されたインタフェースを持つメモリカードとされる。フラッシュメモリカード６５は、特に制限されないが、ローカルメモリとカードコントローラを備え、両者はローカルバスで接続され、全体としてカード基板に構成されてている。ローカルメモリは、特に制限されないが、図１又は図８に示される構成のフラッシュメモリが複数個結合されて成る。上記カードコントローラは、上記ＪＥＩＤＡに適合するインタフェースを介して外部から上記フラッシュメモリを制御する。

【００５１】このようなフラッシュメモリカード６５にも、上記フラッシュメモリ１０を適用することができ、その場合においても、上記実施例の場合と同様の作用効果を有する。

【００５２】以上の説明では主として本発明者によってなされた発明をその背景となった利用分野であるコンピュータシステムに適用した場合について説明したが、本発明はそれに限定されるものではなく、各種データ処理装置に広く適用することができる。

【００５３】本発明は、少なくともメモリセルアレイを含むことを条件に適用することができる。

【００５４】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば下記の通りである。

【００５５】すなわち、レジスタに書込まれたパスワードと、外部から入力されたパスワードとを比較する比較手段の比較結果に基づいて、上記メモリセルアレイからのデータ読出し動作を許可するか否かが判定されるとにより、半導体メモリチップ内部において機密保護機能を実現することができる。

【００５６】レジスタへのパスワード設定が成功したか否かの情報を外部ピンを介して外部出力することができるので、パスワード設定が行われたか否かの確認のため、レジスタの記憶内容を外部出力する必要が無い。それにより、不正ユーザによるパスワード読出しの防止を図ることができる。

【００５７】レジスタへの不適切なパスワード書込みの回数を計数する第１計数手段と、この第１計数手段の計数結果が、所定値に達したか否かを判定するための第１計数値判定手段と、上記第１計数手段の計数結果が所定値に達した場合の処理を、フラグ状態に基づいて決定するための第１フラグ判定手段とが形成されることにより、半導体記憶装置における機密保護機能のためのパスワード設定を的確に行うことができる。

【００５８】不正なパスワードの入力回数を計数する第２計数手段と、この第２計数手段の計数結果が、所定値に達したか否かを判定するための第２計数値判定手段と、上記第２計数手段の計数結果が所定値に達した場合の処理を、フラグ状態に基づいて決定するための第２フラグ判定手段とが形成されることにより、半導体記憶装置における機密保護機能を容易に実現することができる。

【００５９】さらに、上記効果を有する半導体記憶装置と、それをアクセス可能な中央処理装置とを含むデータ処理装置においては、フラッシュメモリ自体で機密保護機能が実現されることから、このフラッシュメモリの記憶情報についての機密保護をシステム的に実現する必要が無いので、システム構成の簡略化を図ることができる。

【図面の簡単な説明】

【図１】図１は本発明の一実施例としてのフラッシュメモリの構成例ブロック図である。

【図２】上記フラッシュメモリに含まれるＭＰＵの機能ブロック図である。

【図３】上記フラッシュメモリにおけるパスワード設定に関する主要部の動作タイミングである。

【図４】上記フラッシュメモリにおけるパスワード設定に関する主要部の動作タイミングである。

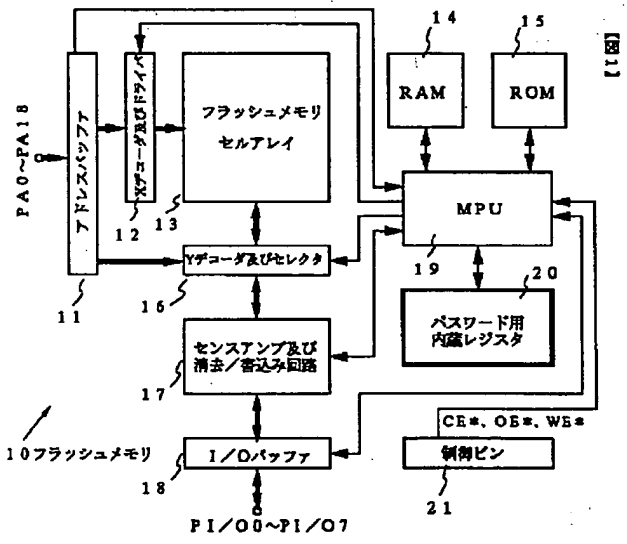
【図５】上記フラッシュメモリにおけるパスワード書込みに関する処理のフローチャートである。

【図６】上記フラッシュメモリにおけるパスワード判定に関する処理のフローチャートである。

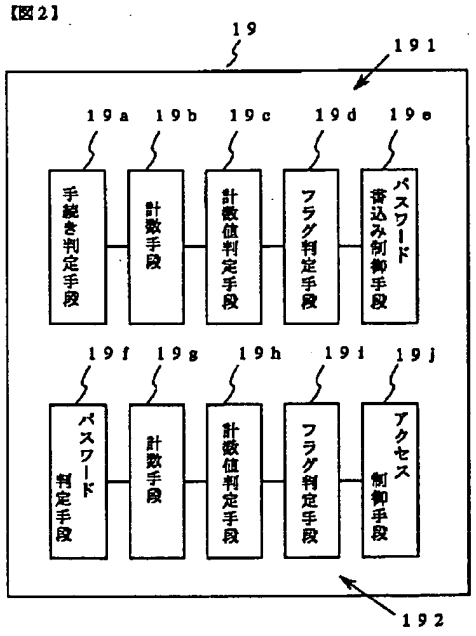
【図７】上記フラッシュメモリを含むデータ処理装置の

全体的な構成例ブロック図である。
【図8】上記フラッシュメモリの他の構成例ブロック図である。
【図9】上記フラッシュメモリの別の適用例であるデータ処理装置の構成例ブロック図である。
【符号の説明】
10　フラッシュメモリ
11　アドレスバッファ
12　Xデコーダ及ドライバ
13　フラッシュメモリセルアレイ
14，62　RAM
15，64　ROM
16　Yデコーダ及びセレクタ
17　センスアンプ及び消去／書込み回路
18　I／Oバッファ
19　MPU
19a　手続き判定手段
19b，19g　計数手段
19c，19h　計数値判定手段
19d，19i　フラグ判定手段
19e　パスワード書込み制御手段
19f　パスワード判定手段
19j　アクセス制御手段
20　パスワード用内蔵レジスタ
21　制御ピン
31　CPU
33　SRAM
34　ROM
35　周辺装置制御部
36　表示制御部
38　外部記憶装置
39　キーボード
40　CRTディスプレイ
51　パスワード誤入力回数カウンタ
61　CPU
62　RAM
63　ROM
64　インタフェース回路
65　フラッシュメモリカード
66　バス

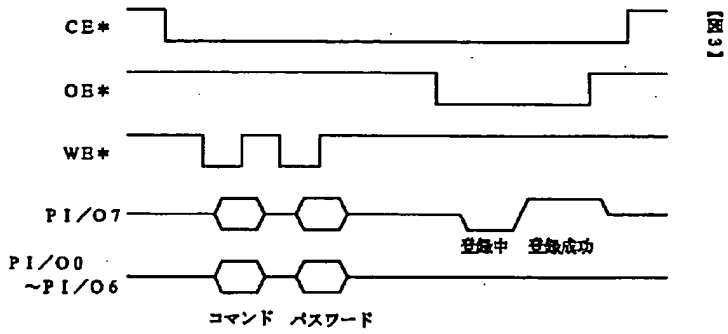
【図1】



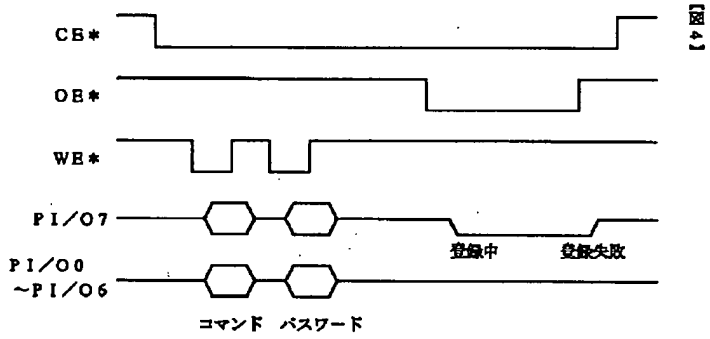
【図2】



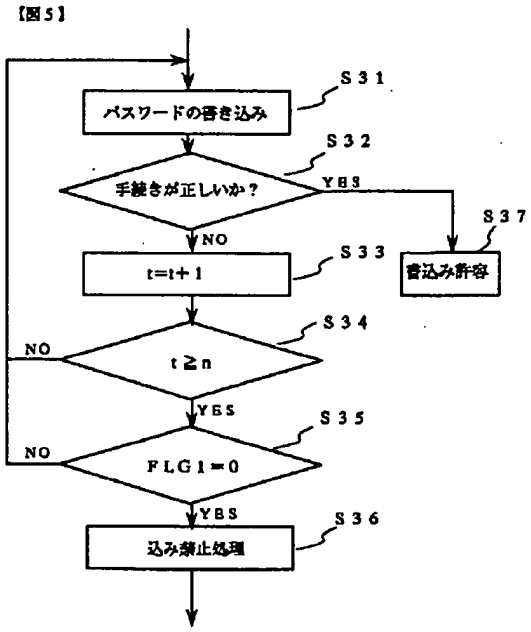
【図3】


【図3】
CE*
OE*
WE*
PI/O7
登録中
登録成功
PI/O0
~PI/O6
コマンド
パスワード

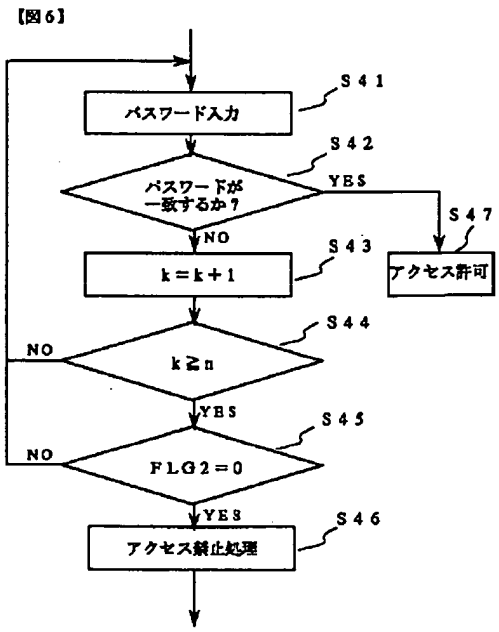
【図4】


【図4】
CE*
OE*
WE*
PI/O7
登録中
登録失敗
PI/O0
~PI/O6
コマンド
パスワード

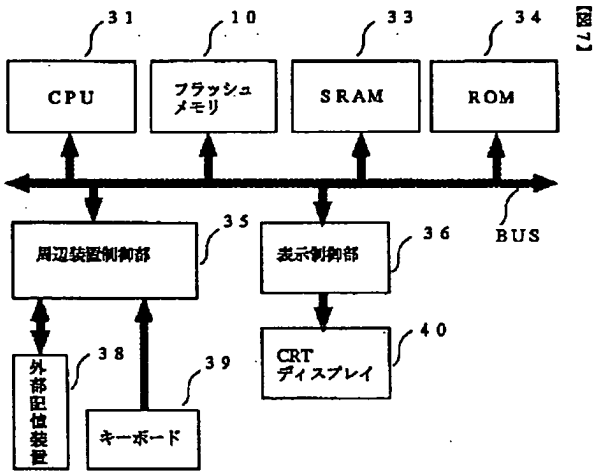
【図5】


【図5】
パスワードの書き込み
S31
手続きが正しいか？
S32
YES
NO
t=t+1
S33
書込み許容
S37
t≧n
S34
NO
YES
FLG1=0
S35
NO
YES
込み禁止処理
S36

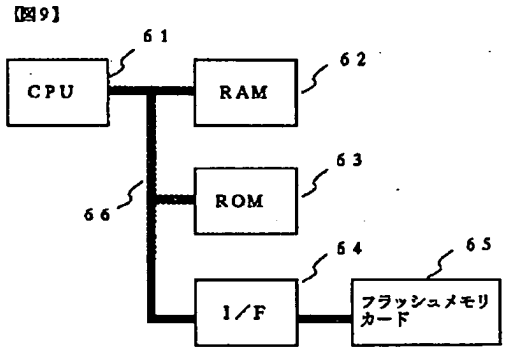
【図6】


【図6】
パスワード入力
S41
パスワードが
一致するか？
S42
YES
NO
k=k+1
S43
アクセス許可
S47
k≧n
S44
NO
YES
FLG2=0
S45
NO
YES
アクセス禁止処理
S46

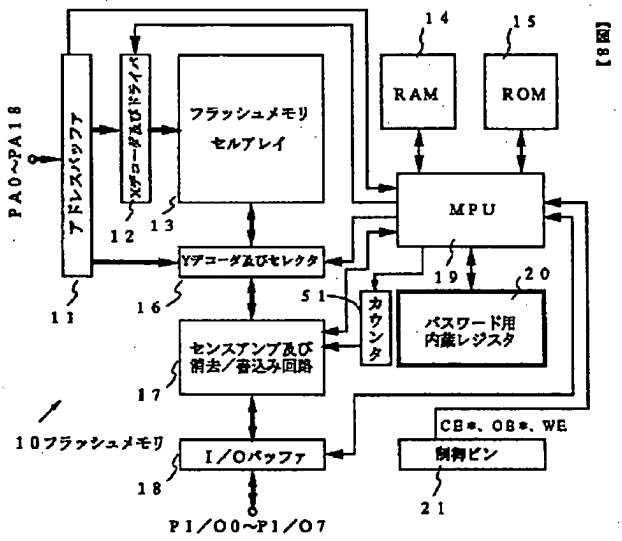
【図7】



【図9】



【図8】



フロントページの続き

(72)発明者　伊澤　和人
東京都小平市上水本町５丁目20番１号　株式会社日立製作所半導体事業部内

(72)発明者　湯川　洋介
東京都小平市上水本町５丁目20番１号　株式会社日立製作所半導体事業部内

(72)発明者　小堺　健司
東京都小平市上水本町５丁目20番１号　株式会社日立製作所半導体事業部内